TLP: WHITE
Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
12/15/2015
12/22/2015 - UPDATED
3/22/2016 - UPDATED

SUBJECT:
Vulnerability in Apache Commons Collections Could Allow Arbitrary Code Execution

OVERVIEW:
A vulnerability has been discovered in Apache Commons Collections which could allow for remote code execution. Apache Commons Collections are a set of implementations, interfaces, and utilities to expand on the functionality of the Java Development Kit (JDK) classes. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the application account and allow for the execution of arbitrary code.

December 22 – UPDATED OVERVIEW:
Additional vulnerabilities have been reported in VMware products that could allow for remote code execution.

March 22 – UPDATED OVERVIEW:
Additional vulnerabilities have been reported in HP Service Manager which could allow for remote code execution.

THREAT INTELLIGENCE:
There are currently no reports of this vulnerability being exploited in the wild. There are known proof-of-concept exploits for this vulnerability.

SYSTEMS AFFECTED:
The following vendors have been found to have products affected by this vulnerability:
- Cisco:http://msisac.cisecurity.org/advisories/2015/2015-149.cfm
- Apache TomEE:http://www.zerodayinitiative.com/advisories/ZDI-15-638/

December 22 – UPDATED SYSTEMS AFFECTED:
- VMware: http://www.vmware.com/security/advisories/VMSA-2015-0009.html

March 22 – UPDATED SYSTEMS AFFECTED:
- *HP Service Manager 9.30 - HP Service Manager 9.41*

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:
A vulnerability has been discovered in the Apache Commons Collections' InvokeTransformer class that when used together with an endpoint that accepts serializable objects can cause remote code execution. This vulnerability could be exploited by de-serializing a specially crafted Java object to execute a payload of arbitrary code on the affected system.

Successful exploitation could result in an attacker gaining the same privileges as the process on the system. Depending on the privileges associated with the process, an attacker could perform actions such as install programs; view, change, or delete data; or create new accounts with full user rights, dependent on the vulnerable application.

December 22 – UPDATED TECHNICAL SUMMARY
Multiple VMware Products are prone to a remote code-execution vulnerability because they fail to properly perform the deserialization on input Java objects. Successful exploit could allow execution of arbitrary commands via a crafted serialized Java object. Exploitation of the issue on vRealize Operations and vCenter Operations is limited to local privilege escalation.

There are currently patches available for vRealize Orchestrator 6.x and vCenter Orchestrator 5.x. Patches for vRealize Operations 6.x, vCenter Operations 5.x, and vCenter Application Discovery Manager are awaiting release.

March 22 – UPDATED TECHNICAL SUMMARY
HP Service Manager is vulnerable to a remote code execution vulnerability. Specifically, this issue occurs because it fails to properly perform deserialization on input Java objects. HP Service Manager is an IT helpdesk application available for multiple platforms.

Successful exploitation of this vulnerability would result in remote code being run within the context of the affected application. Updates are available which mitigate this vulnerability.

RECOMMENDATIONS:
The following actions should be taken:
- Apply vendor-specific updates once they become available after appropriate testing.
- Verify no unauthorized system modifications have occurred on the system before applying patches.
- Monitor intrusion detection systems for any signs of anomalous activity.

REFERENCES:

Cisco:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151209-java-deserialization

Apache:
https://issues.apache.org/jira/browse/COLLECTIONS-580

foxglovesecurity:
http://foxglovesecurity.com/2015/11/06/what-do-weblogic-websphere-jboss-jenkins-opennms-and-your-application-have-in-common-this-vulnerability/

ZDNet:
http://www.zdnet.com/article/java-unserialize-remote-code-execution-hole-hits-commons-collections-jboss-websphere-weblogic/

Infoq:
http://www.infoq.com/news/2015/11/commons-exploit

December 22 – UPDATED REFERENCES:
VMware:
http://www.vmware.com/security/advisories/VMSA-2015-0009.html

March 22 – UPDATED REFERENCES:
HP:
https://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05054565